

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

199.9799 ETH from WhiteBit account
containing Ethereum address
0xE6d503962cE577279EEBf54FfDCD2536
FAbB6401,

Defendant *in Rem*.

No. 3:24-CV-

VERIFIED COMPLAINT FOR FORFEITURE IN REM

Pursuant to Supplemental Rule G(2) of the Federal Rules of Civil Procedure, the United States of America alleges this *in rem* complaint for forfeiture against 199.9799 ETH from WhiteBit account containing Ethereum address 0xE6d503962cE577279EEBf54FfDCD2536FAbB6401 (“Defendant Property”):

NATURE OF THE ACTION

1. This is a forfeiture action under 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C). The United States seeks the forfeiture of the Defendant Property under 18 U.S.C. § 981(a)(1)(A) because it is property involved in a transaction or attempted transaction in violation of section 1956, 1957, or 1960 of Title 18, or property traceable to such property. The Defendant Property also is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C) because it is property that constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (relating to wire fraud), a specified unlawful activity as defined in 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this matter under 28 U.S.C. §§ 1345 and 1355(a), and *in rem* jurisdiction is proper under 28 U.S.C. § 1355(b).

3. Venue in this Court is proper under 28 U.S.C. §§ 1355(b)(1)(A) and 1391(b) because acts or omissions giving rise to the forfeiture occurred in the Northern District of Texas and a substantial part of the events giving rise to the forfeiture occurred in the Northern District of Texas.

PARTIES

4. The Plaintiff is the United States of America.

5. The Defendant Property is 199.9799 ETH from WhiteBit account containing Ethereum address 0xE6d503962cE577279EEBf54FfDCD2536FAbB6401. The Defendant Property was seized from WhiteBit after a federal magistrate judge in the Northern District of Texas signed a seizure warrant for the Defendant Property on April 12, 2024. WhiteBit subsequently transferred the property from WhiteBit account containing Ethereum address 0x17a705346Bb6769b932C41705e1ee1A1f697E989 and 0x26242d87140e17d637553AA1920b22947F6E3711 (the “Subject Accounts”) to a government-controlled wallet held at ETH address 0xE6d503962cE577279EEBf54FfDCD2536FAbB6401.

FACTS

6. The primary responsibility of the Federal Bureau of Investigation (“FBI”) is to identify, investigate, and prevent criminal activity. FBI’s investigations are wide ranging and include cyber and financial crime. The FBI Dallas Division Cyber Squad is

responsible for investigating violations of federal law involving computers and related technologies, including network breaches, malicious software activity, and Internet-related fraud.

7. Investigators, special agents, and task force officers with FBI are specially trained and learn by experience how to identify, investigate, and prevent criminal activity.

8. In late February 2024, the FBI received information from Consensus, a business based in the Northern District of Texas dealing in the purchase, sale, and exchange of virtual currency regarding a fraud scheme that diverted the equivalent of approximately \$1.6M of virtual currency to an unknown subject(s).

9. It is commonplace in cryptocurrency transactions for the sending entity to conduct a “test transaction” to its intended recipient. The test transaction is generally a very small amount, typically the equivalent of \$1 USD. Following this test transaction, the intended recipient returns the exact same value back to the original sender as a way to validate that the test was received and sent to the correct address.

10. Nefarious online actors have discovered this common validation method and have developed techniques to intend to defraud cryptocurrency users by imitating the intended recipient through what is known as an “address poisoning attack”.

11. Once these test transactions are identified, nefarious actors will then utilize a virtual currency address that appears similar to the intended recipient and send the exact amount of the test transaction back to the original sender in an attempt to imitate the intended recipient.

12. Once the original sender observes that their test transaction appears to be legitimized by the return of the funds, the sender then initiates the intended, larger transaction to the address held by the nefarious actors.

13. On or about February 20, 2024, Consensys, while in the course of normal business, was attempting to conduct a transaction in virtual currency to a known entity. Consensys followed its normal procedures and conducted a test transaction to the intended recipient of the equivalent value of \$1 USD.

14. Consensys received the test transaction value back and believed it had verified the intended recipient. However, Consensys fell victim to an address poisoning attack.

15. Consensys initiated a cryptocurrency transaction of 1,698,335 US Dollar Coin (USDC)¹ equivalent to \$1,698,335 USD to the address controlled by the bad actor who had completed the test transaction, 0xa9368b3e4a78ca33aa8ebf4b33535bd65d62011e, (“Theft Address”). Shortly after completing the transaction, Consensys discovered that the funds were inadvertently sent to this impersonator address.

16. Consensys immediately launched an investigation to trace the funds. Analysis of the flow of the funds identified that the funds were divided into several smaller transactions.

¹ US Dollar Coin, or “USDC” is considered a “stable coin” meaning that its value is directly tied to the US Dollar, thus its value is “stable” and not subject to the price instability of other virtual currencies.

17. The FBI conducted its own analysis of the transactions and observed that in less than four hours after the theft, the individual(s) controlling the Theft Address initiated fifteen (15) separate withdrawals. Amongst those transactions were two separate transactions to the Subject Accounts at WhiteBit² totaling 199.99 ETH (Ethereum).

18. On February 20, 2024 at approximately 18:04 UTC (“Transaction 1”), a WhiteBit user attempted to convert 99.99 ETH into Monero (“XMR”), another type of virtual currency. The second transaction (“Transaction 2”), took place on February 20, 2024 at approximately 18:20 UTC in which the same WhiteBit user attempted to convert an additional 99.9899 ETH into Monero.

19. Ultimately, the conversions were not successful as WhiteBit stopped the attempted transactions.

20. Consensus contacted WhiteBit regarding the transaction and WhiteBit was able to freeze 199.9799 ETH.

21. WhiteBit provided information on the WhiteBit user that initiated the ETH to XRM transaction; specifically that the user provided a Ukrainian passport in the name of Dmytro Igorovich Poliatykin.

22. FBI obtained a federal seizure warrant for the 199.9799 ETH held in the Subject Accounts.

² WhiteBit is a cryptocurrency exchange headquartered in Lithuania.

23. After receiving the federal search warrant, WhiteBit transferred the 199.9799 ETH from the Subject Accounts to a government-controlled wallet at address 0xE6d503962cE577279EEBf54FfDCD2536FAbB6401.

24. No claim to the Defendant Property has been filed by Dmytro Igorovich Poliatykin.

FIRST CAUSE OF ACTION
18 U.S.C. § 981(a)(1)(C)
(forfeiture of property related to wire fraud)

25. The United States of America reasserts all allegations previously made.

26. Under 18 U.S.C. § 981(a)(1)(C), any property that constitutes or is derived from proceeds traceable to an offense constituting a “specified unlawful activity,” or a conspiracy to commit such offense, is subject to forfeiture to the United States of America.

27. Under 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1), wire fraud in violation of 18 U.S.C. § 1343 is a “specified unlawful activity.”

28. The wire fraud statute, 18 U.S.C. § 1343, establishes criminal liability for

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

29. As set forth above, money in the form of ETH cryptocurrency was fraudulently obtained through misrepresentations of an address poisoning attack which impersonated the receiving address to divert Consensys’s funds to the Theft Address.

30. As set forth above, the Defendant Property is property that constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343. The Defendant Property is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

SECOND CAUSE OF ACTION
18 U.S.C. § 981(a)(1)(A)
(forfeiture of property related to money laundering)

31. The United States of America reasserts all allegations previously made.

32. Under 18 U.S.C. § 981(a)(1)(A), “[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property” is subject to forfeiture.

33. Under the money laundering statute, 18 U.S.C. § 1956, it is unlawful for any person to conduct or attempt to conduct a financial transaction that involves the proceeds of specified unlawful activity where the person knows the property involved in the financial transaction represents the proceeds of some unlawful activity, and where the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the specified unlawful activity.

34. Under 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1), wire fraud in violation of 18 U.S.C. § 1343 is a “specified unlawful activity” for purposes of the money laundering statute.

35. As set forth above, a financial transaction involving the proceeds of a specified unlawful activity (wire fraud) occurred when cryptocurrency was removed from the Theft Address and, by means of a wire transfer, was deposited into WhiteBit Subject Accounts.

36. Less than four hours after the theft from Consensys, the individual(s) controlling the Theft Address initiated fifteen (15) separate withdrawals in an attempt to conceal the unlawful transactions.

37. As set forth above, the Defendant Property is property involved in a financial transaction or attempted financial transaction in violation of 18 U.S.C. § 1956, or property traceable to such property, and, therefore, the Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

REQUEST FOR RELIEF

WHEREFORE, the United States of America respectfully asserts that the Defendant Property is forfeitable to the United States of America under 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

The United States of America further requests:

- A. That, pursuant to the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, Rule G(3)(b), the Clerk of the Court issue a Summons and Warrant of Arrest *in Rem* as to the Defendant Property;
- B. That Notice of this action be given to all persons known or thought to have an interest in or right against the Defendant Property;
- C. That a Judgment of Forfeiture be decreed against the Defendant Property;

- D. That, upon the issuance of a Judgment of Forfeiture, the United States Marshals Service or its delegate be able to dispose of the Defendant Property according to law; and
- E. That the United States of America receives its costs of court and all further relief to which it is entitled.

DATED this __8__ day of October 2024.

Respectfully submitted,

LEIGHA SIMONTON
UNITED STATES ATTORNEY

/s/ Elyse Lyons
ELYSE LYONS
Assistant United States Attorney
Texas Bar No. 24092735
1100 Commerce Street, Suite 300
Dallas, Texas 75242
Telephone: 214-659-8600
Facsimile: 214-659-8805
Email: elyse.lyons@usdoj.gov

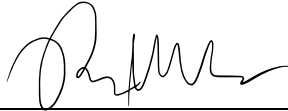
ATTORNEY FOR PLAINTIFF

VERIFICATION

I am a Task Force Officer with the Federal Bureau of Investigation (“FBI”). As a Task Force Officer with FBI, my duties and responsibilities include participating in the investigation and prosecution of persons who violate federal laws.

I have read the contents of the foregoing Verified Complaint for Forfeiture *In Rem* and verify under penalty of perjury pursuant to 28 U.S.C. § 1746 that the factual statements contained therein are true and correct to the best of my knowledge and belief.

Executed this __8__ day of October 2024.

A handwritten signature in black ink, appearing to read 'Ryan Weydeck', is written above a horizontal line.

TFO Ryan Weydeck
Federal Bureau of Investigation